Data Processing Agreement

This Data Processing Agreement (the "**DPA**") is effective _____ ("**Effective Date**") and is made by and between Celona, Inc., ("**Celona**") and _____ ("**Customer**") and is subject to the End User Agreement located at https://Celona.io/eua (the "**Agreement**").

This DPA is incorporated into the Agreement between Celona and Customer and applies to Celona's Processing of Personal Data in connection with Celona's provision of the Products (as defined in the Agreement) to Customer. In the event of any inconsistency between the DPA and the Agreement as to Celona's Processing of Personal Data, the DPA shall control.

---

1. **DEFINITONS**

1.1 In this DPA, the terms "**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in applicable Data Protection Laws with the same or equivalent terms, and the following words and expressions shall have the following meanings unless the context otherwise requires:

1.2 "**Customer Personal Data**" means the Personal Data described in **Appendix 1** of **Exhibit 1**, and any other Personal Data that Celona Processes on behalf of Customer in connection with Celona's provision of the Products.

1.3 "**Data Protection Laws**" means all applicable laws, rules and regulations relating to the Processing of Personal Data as amended, repealed, consolidated or replaced from time to time.

1.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Data by Celona that compromises the security, confidentiality or integrity of such Customer Personal Data.

1.5 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.6 "**Subprocessor**" means any Processor engaged by Celona to Process Customer Personal Data on Celona's behalf.

1.7 "**Third Country**" means any destination country outside of a source country in which the Data Protection Laws restrict transfers of Personal Data to such other destination countries, except where the Data Protection Laws and applicable regulatory authorities of the source country adopted an adequacy decision regarding the Data Protection Laws of the destination country such that transfers of Personal Data to that destination country are not restricted.

1.8 "**UK Addendum**" means United Kingdom ("UK") Information Commissioner's ("ICO") International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0 in force 21 March 2022.

Capitalized terms used in this DPA and not defined above shall have the meaning set forth in the Agreement.

2. DATA PROCESSING

2.1 Celona will only Process Customer Personal Data in accordance with the Agreement (including any order form), and Customer's written instructions, to the extent necessary to provide the Products to Customer, including with respect to transfers of Customer Personal Data, unless Processing is required by other applicable laws, in which case Celona shall, to the extent permitted by applicable law, inform Customer of that legal requirement before so Processing that Customer Personal Data. Celona shall not Process Customer Personal Data outside of the direct business relationship between Customer and Celona. Celona shall not 'sell' or 'share' (as such terms may be specifically defined in applicable Data Protection Laws) Customer Personal Data. The Agreement (including any order form) and the DPA shall be Customer's complete and final instructions to Celona in relation to the Processing of Customer Personal Data. Processing outside the scope of the foregoing will require prior written agreement between Customer and Celona on additional instructions for Processing and may be subject to additional fees.

2.2 Customer shall provide all applicable notices to Data Subjects required under applicable Data Protection Laws for the lawful Processing of Customer Personal Data by Celona in accordance with the Agreement. Customer shall obtain and maintain throughout the term of the Agreement any required consents and/or authorizations related to its provision of, and Celona's processing of, Customer Personal Data as part of the Products. If Customer is not required by Data Protection Laws to obtain and maintain valid consent from Data Subjects, Customer will otherwise obtain and maintain a valid legal basis in accordance with Data Protection Laws to Process Customer Personal Data and for providing such data to Celona for Processing under the Agreement.

2.3 For the avoidance of doubt, Customer's instructions for the processing of Customer Personal Data shall comply with the Data Protection Laws. Customer acknowledges that Celona is reliant on Customer for direction as to the extent to which Celona is entitled to use and Process Customer Personal Data. Consequently, Celona will not be liable for any claim brought against Celona by a Data Subject arising from any act or omission by Celona to the extent that such act or omission resulted from Customer's instructions or Customer's use of the Products.

2.4 Unless otherwise expressly permitted by Celona, Customer Personal Data shall not include any sensitive or special data that imposes specific data security or data protection obligations on Celona in addition to or different from those specified in Agreement or which are not provided as part of the Products.

2.5 If applicable Data Protection Laws recognize the roles of Controller and Processor as applied to Customer Personal Data then, as between Customer and Celona, Customer acts as Controller and Celona acts as a Processor (or Subprocessor, as the case may be) of Customer Personal Data.

2.6 As required by applicable Data Protection Laws, if Celona believes any Customer instructions to Process Customer Personal Data will violate applicable Data Protection Laws, or if applicable Data Protection Laws require Celona to process Customer Personal Data relating to data subjects in a way that does not comply with Customer's documented instructions, Celona shall notify Customer in writing, unless applicable Data Protection Laws prohibit such notification,

provided Celona is not responsible for performing legal research or providing legal advice to Customer.

2.7 Celona shall Process Customer Personal Data for the duration of the provision of the Products in accordance with the Agreement and thereafter only as set forth in the Agreement and this DPA.

2.8 Each party will comply with Data Protection Laws applicable to such party in connection with the Agreement and this DPA.

3. SUBPROCESSORS

3.1 Consent to Subprocessor Engagement. Customer generally authorizes the engagement of third parties as Subprocessors provided such engagement complies with this Section 3. For the avoidance of doubt, this authorization constitutes Customer's prior written consent to the subprocessing of Customer Personal Data for purposes of Clause 9, Option 2 of the Standard Contractual Clauses and any similar requirements of other data transfer mechanisms.

3.2 Information about Subprocessors. A current list of Subprocessors is available here ("Subprocessor List") and may be updated by Celona from time to time in accordance with this DPA. Celona will provide notice of additions to the Subprocessor List via email to Customer.

3.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Celona will:

(a) execute with Subprocessors a written agreement providing:

(i) the Subprocessor only Processes Customer Personal Data only to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement and this DPA; and

(ii) the Subprocessor utilize the same level of data protection and security with regard to its Processing of Customer Personal Data as are described in this DPA.

(b) be responsible for the Subprocessor's violations of this DPA or Data Protection Laws in relation to the services such Subprocessor provides to Celona to the extent Celona would be liable for the same violations under the terms of the Agreement.

3.4 Opportunity to Object to Subprocessor Changes**.** Customer may, on reasonable and objective grounds, object to Celona's use of a new Subprocessor by providing Celona with written notice within fifteen (15) days after Celona has provided notice to Customer as described herein with documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA or Data Protection Laws ("Objection"). In the event of an Objection, Customer and Celona will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Data Protection Laws. To the extent Customer and Celona do not reach a mutually acceptable resolution within a reasonable timeframe, Celona will use reasonable endeavors to make available to Customer a change in the Products or will recommend a commercially reasonable change to the Products to prevent the applicable Subprocessor from Processing Customer Personal Data. If Celona is

unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, Customer shall have the right to terminate Celona's provision of the relevant Products (i) in accordance with the termination provisions in the Agreement; (ii) without liability to Customer or Celona, and (iii) without relieving Customer from its payment obligations under the Agreement up to the date of termination.

4. INTERNATIONAL TRANSFERS

4.1 In accordance with Customer's instructions under Section 2, Celona may Process Customer Personal Data on a global basis as necessary to provide the Products, including for IT security purposes, maintenance and provision of the Products and related infrastructure, technical support, and change management.

4.2 To the extent that the Processing of Customer Personal Data by Celona involves the transfer of such Customer Personal Data from a country whose Data Protection Laws restrict the transfer of Personal Data to Third Countries, then such transfers shall be subject to the protections and provisions of the Standard Contractual Clauses (for which the SCC Appendix is attached to this DPA in Schedule 1), the UK Addendum for transfers from the UK to Third Countries, or other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Data Protection Laws.

4.3 Customer shall be deemed to have signed the SCC in Schedule 1, Annex I in its capacity of "data exporter" and Celona in its capacity as "data importer." Module Two or Module Three of the Standard Contractual Clauses shall apply to the transfer depending on whether Customer is Controller of the Personal Data (for Module Two) or a Processor of the Personal Data on behalf of its customer (for Module Three). If Module Three applies, Customer hereby notifies Celona that it is a Processor and the instructions shall be as set forth in this DPA. For purposes of Clauses 17 and 18 of the SCCs, the Parties select the Netherlands. Clause 7 is omitted. In Clause 11(a), the optional provision shall not apply. Additional provisions applicable to customer Personal Data transferred pursuant to SCC are set forth in Schedule 2. To the extent such a transfer includes Personal Data subject to Data Protection Laws of Switzerland, the Standard Contractual Clauses shall be adapted to use for Switzerland (where the Swiss Federal Act on Data Protection shall apply as the applicable Data Protection Law, Clauses 17 and 18 of the SCCs shall refer to Switzerland, and Data Subjects in Switzerland shall be able to avail themselves of any rights conferred by the Standard Contractual Clauses).

4.4 The SCC, or UK Addendum, as applicable, will cease to apply if Celona has implemented an alternative recognized compliance mechanism for the lawful transfer of personal data in accordance with applicable Data Protection Laws.

4.5 In the event of any conflict between any terms in the SCC or UK Addendum, as applicable, and the DPA, the SCC or UK Addendum, as applicable, shall prevail to the extent of the conflict.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 Celona Security Obligations**.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Celona shall implement appropriate technical and organizational measures designed to ensure a level of

security appropriate to the risk of the Processing, including the measures set out in Schedule 1. Celona may update its security practices from time to time but will not materially decrease the overall security of the Products during the term of the Agreement. Such measures shall include process for regularly testing, assessing, and evaluating the effectiveness of the measures.

5.2 Security Audits.

(a) Celona will, upon Customer's written request, verify its compliance with its obligations in this DPA by first providing to Customer for its review documentation regarding the same and, if such documentation is not reasonably sufficient to address Customer's inquiries, participate in and contribute to audits as set forth below.

(b) Customer may, upon at least 30 days' advance written notice and at reasonable times, audit (either by itself or using independent third-party auditors) Celona's compliance with the security measures set out in this DPA solely for the purpose of confirming Celona's compliance with its obligations under this DPA. Celona shall reasonably assist with any audits conducted in accordance with this Section 5.2. Such audits may be carried out once per year, or more often if required by Data Protection Law or Customer's applicable Supervisory Authority.

(c) Any third party engaged by Customer to conduct an audit must be pre-approved by Celona (such approval not to be unreasonably withheld) and sign Celona's confidentiality agreement. Customer must provide Celona with a proposed audit plan at least two weeks in advance of the audit, after which Customer and Celona shall discuss in good faith and finalize the audit plan prior to commencement of audit activities.

(d) Audits may be conducted only during regular business hours, in accordance with the finalized audit plan and Celona's security and other policies and may not unreasonably interfere with Celona's regular business activities. Celona is not required to grant access to its premises or systems for the purposes of such an audit to any individual unless they produce reasonable evidence of identity and authority. Customer shall reimburse Celona for any costs or expenses incurred by Celona in connection with the Audit or with granting access to its data processing facilities.

(e) Information obtained or results produced in connection with an audit are Celona confidential information and may only be used by Customer to confirm compliance with this DPA and for complying with its requirements under Data Protection Laws.

(f) In lieu of Customer auditing a Subprocessor, Customer may request that Celona audit a Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Customer in obtaining a third-party audit report concerning the Subprocessor's operations) to verify compliance with the Subprocessor's obligations.

(g) Without prejudice to the rights granted in Section (b) above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report or attestation letter issued by a qualified third party auditor within the prior twelve months and Celona provides such report or attestation letter to Customer confirming there are no known material changes in the controls audited, Customer agree to accept the findings presented in the third party audit report or attestation letter in lieu of requesting an audit of the same controls covered by the report.

5.3 Upon Customer's written request, Celona shall make available all information reasonably necessary to demonstrate compliance with this DPA as required by Data Protection Laws.

5.4 Personal Data Breach Notification.

(a) If Celona or any Subprocessor becomes aware of and determines a Personal Data Breach has occurred, Celona will:

(i) notify Customer of the Personal Data Breach without undue delay and, in any event, within 48 hours after such determination, at the contact information on file, where such notification shall describe (1) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (2) the reasonably anticipated consequence of the Personal Data Breach; (3) measures taken to mitigate any possible adverse effects; and (4) other information concerning the Personal Data Breach reasonably known or available to Celona that Customer is required to disclose to a Supervisory Authority or Data Subjects under Data Protection Laws; and

(ii) investigate the Personal Data Breach and provide such reasonable assistance to the Client (and any law enforcement or regulatory official) as required to investigate the Personal Data Breach.

5.5 Except as required by applicable Data Protection Laws, the obligations set out in Section 5.4 shall not apply to Personal Data Breaches caused by Customer.

5.6 Celona's contact point for additional details regarding a Personal Data Breach is privacy@celona.io. Celona's provision of any notification of a Personal Data Breach shall not constitute an admission of fault.

5.7 Customer is solely responsible for fulfilling any Personal Data Breach notification obligations applicable to Customer. Customer and Celona shall work together in good faith within the timeframes for Customer to provide Personal Data Breach notifications in accordance with Data Protection Laws to finalize the content of any notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Laws. Celona's prior written approval shall be required for any statements regarding, or references to, Celona made by Customer in any such notifications.

5.8 Celona shall treat Customer Personal Data as the Confidential Information of Customer, and shall put procedures in place to ensure that any employees or other personnel with access to Customer Personal Data have committed themselves to confidentiality of Customer Personal Data or are under an appropriate statutory obligation of confidentiality and do not Process such Customer Personal Data other than in accordance with this DPA.

5.9 Customer is responsible for security relating to its environment and databases and security relating its configuration of the Products. This includes implementing and managing procedural, technical, and administrative safeguards on its software and networks sufficient to: (a) ensure the confidentiality, security, integrity, and privacy of Customer Personal Data in transit, at rest, and in storage; (b) protect against any anticipated threats or hazards to the security and integrity of Customer Personal Data; and (c) protect against any unauthorized processing, loss, use, disclosure or acquisition of or access to Customer Personal Data. Notwithstanding any other provision of this DPA, the Agreement or any other agreement related

to the Products, Celona will have no obligations or liability as to any breach or loss resulting from: (x) Customer's environment, databases, systems or software, or (y) Customer's security configuration or administration of the Products.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 Save as required (or where prohibited) under applicable law, Celona shall promptly notify Customer of any request received by Celona or any Subprocessor from a Data Subject in respect of their Personal Data included in Customer Personal Data ("Data Subject Request") and shall not respond to the Data Subject Request where the Data Subject identifies Customer as its Controller. If a Data Subject does not identify a Controller, Celona will instruct the Data Subject to identify and contact the relevant Controller.

6.2 Where applicable, and taking into account the nature of the Processing, Celona shall use reasonable endeavors to assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to Data Subject Requests as required by Data Protection Laws. In order to receive such assistance, Customer shall utilize any tools provided by Celona including those providing Customer with the ability to correct, delete, block, access or copy the Personal Data of a Data Subject. If such functionality or other tools are not available, Customer may submit a support ticket requesting assistance and clearly stating the nature of the Data Subject Request.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, Celona shall provide reasonable assistance to Customer with any data protection impact assessments and with any prior consultations to any Supervisory Authority of Customer, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to Celona.

7.2 Such cooperation and assistance are provided to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Celona. Celona may fulfil its above obligations by providing Customer with documentation regarding its Processing operations.

8. RETRIEVAL AND DELETION OF PERSONAL DATA

8.1 Upon Customer's written request and no later than the following events: (i) cessation of Processing of Customer Personal Data by Celona; or (ii) ninety (90) days after termination or expiration of the Agreement ("Retrieval Period"), except as otherwise permitted by applicable Data Protection Laws, Celona shall:

(a) make available to Customer a complete copy of Customer Personal Data then available in the Products in electronic format; and

(b) after such Retrieval Period, delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data Processed by Celona or any Subprocessors, and where deletion is not possible, sufficiently de-identify Customer Personal Data such that it is no longer Personal Data, except if required or permitted by applicable law or for legal, compliance, audit, or security purposes.

8.2 Celona may continue to retain and use Customer Personal Data to the extent (1) required by applicable Data Protection Laws for the period as required by Data Protection Laws, and provided that Celona shall ensure the confidentiality of all such Customer Personal Data and that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable Data Protection Laws requiring its storage and for no other purpose or (2) in aggregate or de-identified form without restriction provided the data additionally does not identify Customer.

9. GENERAL

9.1 With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including but not limited to the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations for Customer Personal Data of a Data Subject.

9.2 Celona may share and disclose Customer Personal Data and other data of Customer in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Celona's business by or to another company, including the transfer of contact information and data of customers, partners and end users.

9.3 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, the Parties' authorized representatives have executed this DPA as of the Effective Date.

CUSTOMER: _____		**CELONA, INC.**	
Signed:	_____	Signed:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter

Name:	The data exporter is the entity identified as “Customer” in the DPA
Address:	As set forth in the Agreement
Contact person:	As set forth in the Notices provision in the Agreement
Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA or Agreement, as applicable
Role:	Controller, except when processing data on behalf of another entity, in which case data exporter is a Processor

Data importer

Name:	The data importer is the entity identified as “Celona” in the DPA
Address:	As set forth in the Agreement
Contact person:	
Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA or Agreement, as applicable
Role:	Processor, or Subprocessor if data exporter is a Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Data exporter's personnel who have access to Celona Orchestrator cloud services; and individuals to whom Data exporter provides a SIM card or eSIM for access to Data exporter's private LTE/5G network powered by Celona.
Categories of personal data transferred:	Data exporter's personnel: name, email, telephone number, job title, business address, IP address for Orchestrator user log-ins Individuals Receiving a SIM: IMEI (International Mobile Equipment Identity) number and EID number of connected devices used with Celona private SIMs. SIM data: ICCID and IMSI numbers IP address allocated to devices that connect to the Celona Private Wireless network Application traffic data / IPs
Sensitive categories of data (if appropriate):	N/A
The frequency of the transfer:	As set forth in the Agreement
Nature of the processing:	The subject-matter and nature of the processing of data exporter Personal Data by data importer is for the provision of the Products to the data exporter under the Agreement.
Purposes of the data transfer and further processing:	Refer to DPA.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal Data will be processed for the duration of the Agreement, subject to Section 8 of the DPA

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Refer to DPA and the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority shall be The Netherlands, the UK ICO for matters related to the UK or UK data subjects, or the Swiss Federal Data Protection and Information Commissioner for matters related Switzerland or Swiss data subjects.

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of the Customer Personal Data:

Celona's technical and organizational measures are described in its Security Feature Brief and may be updated from time to time as required as set forth in the Addendum.

The following measures will be implemented:

- **Administrative controls**
  - Security education, training, and awareness program - data importer trains all employees on hire and on a recurring basis on security concepts. Training exercises are conducted to provide opportunities to use their knowledge.
  - Developer security training - Software developers receive additional ongoing training in secure coding concepts.
  - User access reviews - Access to critical systems is reviewed for appropriate authorizations regularly on a recurring basis.
  - Backup strategy - maintain backups consistent with availability and durability requirements.
  - Incident response team - data importer maintains an incident response capability including a specific team to handle such incidents.
  - Secure system development lifecycle - System development follows a documented process and includes security considerations throughout the lifecycle.
  - Change management process - All changes to software go through a documented change management process.
- **Technical Controls**
  - Encryption in transit - Communication with the web application is performed through a TLS-secured connection with a restricted cipher suite.
  - Encryption at rest - data exporter personal data is protected with AES256 encryption and unique keys for each user.
  - Backups - Critical data and system configuration information is backed up on a regular and rolling basis.

    - Vulnerability scanning - Web application scanning occurs regularly to identify potential vulnerabilities within data importer's platform.
    - Static code analysis - Source code is subjected to static analysis to uncover errors or security risks prior to being approved for use in service delivery.
    - Capacity monitoring - Information assets are monitored to ensure capacity exceeds that needed to meet demand.
- **Physical Controls**
    - Infrastructure hosted and secured by Amazon Web Products - data importer infrastructure to deliver services is hosted by Amazon Web Products and includes physical measures designed to protect against fire, flood, power interruption, and sabotage.

ANNEX III

The data exporter has authorized the use of the following subprocessors:

As set forth in Section 3 of the DPA.

SCHEDULE 2 – ADDITIONAL SCC PROVISIONS

BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS 01/2020

1. Government Disclosure Requests.

    a. Celona shall, unless otherwise prohibited by law or a legally binding order of an applicable body or agency, promptly notify Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("**Disclosure Request**") without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request).

    b. Celona will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and to challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, Celona shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Celona shall not disclose Customer Personal Data requested until required to do so under applicable law. Celona shall only provide the minimum amount of Customer Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request.

    c. If the Disclosure Request is incompatible with the SCCs or other data transfer mechanism utilized in accordance with Section 4 in this DPA, Celona will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Customer Personal Data subject to the Disclosure Request.

    d. Celona will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Celona will provide Customer with such records relevant to Customer Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Celona's legal rights in connection with threatened, pending, or current litigation.

2. Celona has, as of the Effective Date, not received any national security orders under Foreign Intelligence Surveillance Act ("FISA") Section 702.

3. As of the Effective Date, no court has found Celona to be the type of entity defined in 50 U.S.C § 1881(b)(4) eligible to receive process issued under FISA Section 702.

4. Celona has not purposefully created "back doors" or similar programming in its systems that provide Products that could be used to access the systems and/or Customer Personal Data, nor has Celona purposefully created or changed its business processes in a manner that facilitates access to Customer Personal Data or its systems that provide the Products. To the best of Celona's knowledge, United States Data Protection Laws do not require Celona to create or maintain "back doors" or to facilitate access to Customer Personal Data or systems that provide Products or for Celona to possess or provide the encryption key in connection with a United States Disclosure Request.

5. Celona shall use reasonable efforts to assist Customer and its Data Subjects, as instructed by Customer (in accordance with Section 6 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Customer in connection with the Data Subject's efforts to exercise its rights and obtain legally available redress, provided Celona shall not be required to provide Customer or Data Subjects with legal advice.

6. Celona has established an internal procedure regarding handling of Disclosure Requests and applicable transfers of Personal Data of customers. Celona has procedures for applicable personnel to receive information, as appropriate, regarding applicable transfers of Customer Personal Data, where such information may include an explanation of the necessity of the transfer and any data protection safeguards in scope.

7. In the event Celona receives a request to voluntarily disclose unencrypted Customer Personal Data to a government authority, Celona will use reasonable efforts to first obtain Customer's consent, either on its behalf or on behalf of the relevant Data Subject.